AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of:

3041 S. 56th Street, Apt. 49, Milwaukee, WI 53219 and any vehicle located on the premises under the control of Brian BRIDGES. See Attachment A.

Case No. 19-M-135

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 922(a)(1)(A)

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Frank Rutter, ATF

Printed Name and Title

Sworn to before me and signed in my presence:

Date: July 8, 2019

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. David E. Jones, U.S. Magistrate Judge

Printed Name and Title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Frank Rutter, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 3041 S. 56th Street, Apartment 49, Milwaukee, WI 53219, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and have been since November 2015. As an ATF Agent, I have conducted and participated in numerous investigations regarding the unlawful possession of firearms by convicted felons in violation of 18 U.S.C. § 922(g)(1). I have conducted firearm investigations involving violations of 18 U.S.C. § 922(a)(6), commonly referred to as "lying and buying." I have also conducted firearms trafficking investigations and participated in those involving subjects dealing firearms without a license in violation of 18 U.S.C. § 922(a)(1). I have had a variety of formal, informal, and on the job training related to investigating subjects suspected of dealing firearms without a license, and I have participated in the execution of search warrants in which firearms and records were seized.

3. The facts in this affidavit come from my personal knowledge and observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. On December 26, 2018, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Milwaukee Field Office received a tip from the Wisconsin Department of Justice that Rahsaan Lewis (DOB: xx/xx1976) had purchased a large quantity of handguns during the month of December 2018.

5. Between December 26, 2018 and January 2, 2019, affiant collected and reviewed ATF Form 4473's related to firearms purchased by Lewis. ATF Form 4473 is a firearm purchase record required by federal law to be completed when a Federal Firearm Licensee (FFL) sells a firearm. This document must be completed by the purchaser in the presence of the FFL from whom they are purchasing the firearm. This document contains a wealth of information including, but not limited to, the purchaser's name, address, and a signed statement affirming they understand that the repetitive purchase of firearms for the purpose of resale for livelihood and profit without a Federal firearms license is a violation of Federal law. Additionally, this document requires the purchaser to attest they are the actual purchaser of the firearm and are not acquiring the firearm on behalf of someone else.

6. ATF records indicated that Lewis did not, and does not, have a federal firearms license.

7. For background, Title 18, United States Code, Section 922(a)(1)(A) provides in relevant part that it is unlawful for any person, "except a licensed importer, licensed manufacturer, or licensed dealer, to engage in the business of . . . dealing in firearms, or in the course of such business to ship, transport, or receive any firearm in interstate or foreign commerce." Title 18, United States Code, Section 924(a)(1)(D) sets forth the penalty for a willful violation of that section. Title 18, United States Code, Section 921(a)(11)(A) defines a "dealer" to mean "any person engaged in the business of selling firearms at wholesale or retail." Title 18, United States Code, Section 921(a)(22) provides that the term "engaged in the business" means, as applied to a dealer in firearms, "a person who devotes time, attention, and labor to dealing in firearms as a regular course of trade or business with the principal objective of livelihood and profit through the repetitive purchase and resale of firearms, but such term shall not include a person who makes occasional sales, exchanges, or purchases of firearms for the enhancement of a personal collection or for a hobby, or who sells all or part of his personal collection of firearms." Title 18, United States Code, Section 921(a)(22), provides in part that the term "with the principal objective of livelihood and profit" means "that the intent underlying the sale or disposition of firearms is predominantly one of obtaining livelihood and pecuniary gain, as opposed to other intents, such as improving or liquidating a personal firearms collection."

8. Records showed that between November 8, 2018, and December 31, 2018, Lewis purchased approximately forty (40) handguns. Many of these firearms were of the same make and model, which is not indicative of someone purchasing firearms for their private collection. Additionally, the firearms purchased were new, low cost models not considered to be antique or collectible firearms.

9. On January 2, 2019, affiant conducted an interview of Lewis at Lewis's residence. During this interview, Lewis explained, among other things, that he was uncertain how many firearms he had purchased since November 2018 but believed it to be approximately twenty five (25) or more.

10. Lewis said he had not been working since January 2018 due to an injury. Lewis stated his worker's compensation payments had stopped in November 2018, which is when he began dealing with firearms because he needed to make money. Lewis said that the money earned from firearm sales was his only source of income.

11. Lewis explained he kept his firearms inside his residence and had sold approximately half of the firearms he had purchased since November 2018. Lewis said he had most recently sold approximately ten (10) firearms at a gun show on 12/14/18. Lewis stated that his nephew had accompanied him, and that he still was in possession of around ten (10) guns that he had purchased in the preceding month.

12. A federal warrant was obtained for the search of Lewis's residence, which was executed on January 11, 2019. Initially, Lewis was not present and, when contacted by phone, said that he sold the remaining firearms in his possession since the January 2, 2019 interview. When Lewis later arrived at the residence, he

provided a different explanation and said that he had given at least two of the remaining firearms to his nephew, "Brian Bridges."

13. Pursuant to the search warrant, Lewis's cellular phones were seized and their contents were examined. The phone extractions contain evidence of communications between Lewis and others regarding firearms purchases. Messages found on the devices show that Lewis purchased firearms with the intention of reselling those firearms to various acquaintances in and around Chicago, Illinois.

14. Lewis's phones also contained evidence of various conversations regarding firearms with an individual using phone number 414-391-0488. This number was saved as "Brian" in one of Lewis's phones.

15. On June 12, 2019, this Court issued an Order requiring Sprint Corporation to disclose certain records pursuant to 18 U.S.C. § 2703(d). *See* App. No. 13028. Documentation obtained from Sprint Corporation shows that telephone number 414-391-0488 was associated with "Alex Bridges" during the relevant time period.

16. Affiant also collected and reviewed ATF Form 4473's related to firearms purchased by BRIDGES. On each of these forms, BRIDGES provided his full name as "Brian Alexander Bridges," and the PREMISES as his address. On at least three forms, he provided his telephone number as 414-391-0488.

17. On November 1, 2018, as Lewis was communicating regarding firearms with a potential customer, he sent a text message to BRIDGES asking if BRIDGES

wanted to go to Chicago with him. Lewis also asked his potential customer whether he was interested in a Mossberg M715P .22 caliber pistol.

18. Later that evening, BRIDGES purchased a Mossberg M715P .22 caliber pistol at Fleet Farm, a federal firearms licensee, in Germantown, Wisconsin. BRIDGES completed ATF Firearm Transaction Form 4473, which was lawfully required to finalize the firearm acquisition from Dunham's. In response to Question No. 11(a), BRIDGES stated that he was the actual buyer of the firearm. The initial background response was delayed, and BRIDGES did not take possession of this weapon until November 8, 2018.

19. On or about November 5, 2018, Lewis's potential customer inquired as to Lewis's status. Lewis responded that he was "waiting on a mini draco" (a term that generally refers to AK-style pistols, which bear some similarity in appearance and form to the Mossberg model purchased by BRIDGES on November 1) that "we" (believed to refer to himself and BRIDGES) ordered. Lewis's potential customer expressed interest in buying two of the Mossberg pistols, and a 4-minute phone call followed. Later that morning, Lewis sent a link to BRIDGES with an online template for a Firearms Bill of Sale. Lewis also later sent a printable template denoted "Wisconsin Gun Bill of Sale."

20. According to firearms transaction records, the Mossberg pistol was transferred to BRIDGES on November 8, 2018, at 1:40 p.m. At or around that time, BRIDGES re-certified that his answers on the ATF Form 4473 remained true, correct, and complete. On November 8 at 2:06 p.m., Lewis informed his potential customer

that he was on his way, and sent a picture that appeared to include the Mossberg pistol purchased and received by BRIDGES. According to firearms transaction records, BRIDGES purchased and received two more Mossberg M715P .22 caliber pistols on November 10, 2018.

21. On the morning of November 16, 2018, BRIDGES purchased and took possession of a Ruger EC9S 9mm pistol and a Taurus G2C 9mm pistol from Dunham's, a federal firearms licensee, in West Allis, Wisconsin. BRIDGES completed ATF Firearm Transaction Form 4473, which was lawfully required to finalize the firearm acquisition from Dunham's. BRIDGES stated on ATF Firearm Transaction Form 4473, Question No. 11(a), that he was the actual buyer of the firearm.

22. On the morning of November 17, 2018, Lewis sent a text message to BRIDGES: "If they don't call me by 10 u should probably go try n get the others..so we can get going." Lewis also told a potential customer that he was trying to bring him firearms that day.

23. At or around 1:26 p.m. on November 17, 2018, BRIDGES purchased two Taurus G2C 9mm pistols from Dunham's, a federal firearms licensee, in West Allis, Wisconsin. BRIDGES completed ATF Firearm Transaction Form 4473, which was lawfully required to finalize the firearm acquisition from Dunham's. BRIDGES stated on ATF Firearm Transaction Form 4473, Question No. 11(a), that he was the actual buyer of the firearms.

24. Notably, Lewis had purchased two of the same model on November 15, but, due to a delayed background response, was unable to take possession of the guns

immediately. Shortly after purchasing the firearms, BRIDGES sent Lewis a text message: "Let's roll!" Lewis asked BRIDGES, "Wut u get" and a phone conversation took place. Subsequent communications to and from Lewis suggest that Lewis drove to Chicago later that day.

25. On December 27, 2018, Lewis received a request for several firearms. Lewis then texted BRIDGES that they "gotta get 5 9s" and included some math: "235×2+115=585 a piece...90 x 5 = 450 ÷ 2=225." On December 28, 2018, BRIDGES sent Lewis a text message asking for an update. Lewis responded he was at Dunham's. A few hours later, Lewis sent a text message to a potential customer explaining that he was in Chicago with 9mm pistols for sale. Shortly thereafter, BRIDGES sent Lewis a text message seeking an update. BRIDGES asked if Lewis had sold four (4) or six (6) firearms. LEWIS responded he had only sold four (4) firearms and that the purchasers were trying to lower the purchase price. BRIDGES responded, "No. The deal is the deal[.]"

26. On December 30, Lewis sent BRIDGES a text message indicating that he had gotten an order that was too large to purchase at once and needed to be broken down into "2 moves," including "4 40s... 1 g2c..1 ec9.. in the morning." Several telephone calls between Lewis and BRIDGES' phones followed.

27. The next day, Lewis sent a text message to BRIDGES explaining that he had "hit Hwy," apparently on his way to Chicago. Lewis later followed up with a text message informing BRIDGES that Lewis's daughter needed to be back in Milwaukee by 1700 hours and the purchaser did not get off work until 2000 hours.

Lewis explained they had to leave the firearms with Lewis's father at his parents' house. BRIDGES responded, "Are u kidding me man ... When we gone get tge [*sic*] money[?]"

28. On June 26, 2019, affiant reviewed information obtained from a public record aggregating company commonly utilized by law enforcement, which revealed the PREMISES as BRIDGES' current listed address. Additionally, affiant was able to verify with property management that BRIDGES was the sole tenant at the PREMISES and had signed a one year lease in November 2018. On the same date, affiant reviewed State of Wisconsin Department of Transportation (WIDOT) information, and BRIDES' driver's license listed the PREMISES as his residence as recent as November 16, 2018.

29. Based on the investigation thus far, there is probable cause to believe that physical evidence associated with firearms dealing in violation of federal law is located at the PREMISES.

30. Further, affiant is aware, based on training, experience, and information provided from other members of law enforcement, that evidence of dealing firearms without a license is commonly found on electronic devices such as computers and cellular phones. Affiant is aware that those engaged in the sale of firearms, especially those like Lewis and BRIDGES, who do not have a brick and mortar business location for selling firearms, communicate and coordinate their activities with others associated with firearms sales. Affiant is aware that those engaged in the sale of firearms often take, or cause to be taken, photographs, video,

and other visual depictions of firearms, and typically keep and maintain these photographs, video, and other visual depictions in cellular phones located on their person or on other mediums such as computers and hard drives in areas where they have exercised dominion and control.

31. Affiant is aware that cellular phones can be used to store information including text messages, multimedia messages, and a history of incoming and outgoing calls, contact/address book information, photographs, videos, GPS and other location information, internet search history, and other data.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

32. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

33. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can

be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

34. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under

investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical

location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are

necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

35. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data

recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

37. *Unlocking Apple brand devices:* I know based on my training and experience, as well as from information found in publicly available materials including those published by Apple, that Apple devices are used by many people in the United States, and that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

a. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found

in the round button (often referred to as the "home" button) at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

b. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

c. If Touch ID enabled Apple devices are found during a search of the PREMISES, the passcode or password that would unlock such the devices are presently unknown to law enforcement. Thus, it will likely be necessary

to press the finger(s) of the user(s) of any Apple device(s) found during the search of the PREMISES to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

d. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the premises to press their finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the PREMISES in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

e. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Apple device(s) found in the PREMISES as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

f. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the PREMISES to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the PREMISES for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

CONCLUSION

38. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A

Property to be searched

The property to be searched is 3041 S. 56th Street, Apt. 49, Milwaukee, WI 53219, as well as any vehicle located on the premises under the control of Brian BRIDGES. The aforementioned property is further described as a two-story apartment complex. The structure is a combination of brown brick and vertical brown siding with some tan accents around the windows. The shared common entryway has the numbers "3041"affixed on the right side of the door. There is a shared underground parking garage beneath the structure and also an open air parking lot to the North.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 922(a)(1)(A), unlawful firearms dealing, involving Brian BRIDGES and occurring after October 1, 2018, including:

a. Firearms, magazines, or ammunition.

b. Records and information relating to the sale or transfer of firearms, including manufacturers' gun boxes and shipping containers, labels and tags regarding pricing and sales, receipts relating to purchases or sales, and ATF forms.

c. Records and information relating to laws or regulations regarding the sale or transfer of firearms.

d. Ledgers, sales and customer lists, supplier information, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when firearms were obtained, transferred, sold, distributed, and/or concealed.

e. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses or communications relating to the unlawful dealing of firearms between LEWIS and any individuals connected to such activities.

f. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities.

g. Records, items and documents reflecting travel for the purpose of participating in the purchase, sale, or transfers of firearms, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, GPS information, internet searches, and records of calls reflecting travel.

h. Indicia of occupancy, residency, or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys.

i. Photographs, videotapes or other depictions of assets, firearms, or accomplices.

j. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from unlawful dealing in firearms, or financial transactions related to unlawful dealing in firearms.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of Apple brand device(s), such as an iPhone or iPad, found at the premises for the purpose of

attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.